GDPR: RUOLI E RESPONSABILITA’

DOTT.SSA LUANA FIERRO

Titolare del trattamento, responsabile della protezione e responsabile del trattamento

webgrafia

- *Regolamento (UE) 2016/679*, https://www.garanteprivacy.it/il-testo-del-regolamento, 1 agosto 2018;

- *Data Protection Officer: perché serve una figura autonoma e indipendente*,

Andrea Lisi, avvocato, Presidente ANORC Professioni; Direttore Master Unitelma La Sapienza; 1-9-2017; https://www.agendadigitale.eu/sicurezza/data-protection-officer-perche-serve-una-figura-autonoma-e-indipendente/

Diritto alla protezione dei dati

- Il diritto alla protezione dei dati personali è un diritto fondamentale, che converge nella tutela dell'identità personale
- Nell'interesse di questo diritto è previsto l'obbligo di nominare il DPO
- ***Sezione 4***
- ***Responsabile della protezione dei dati***
- ***Articolo 37***
- ***Designazione del responsabile della protezione dei dati, par. 1***

Art. 37, par. 1

- *1.Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:*
- ***a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;***

Art. 37, par. 1

- *b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;*

- *oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.*

…Designazione DPO (detto anche: Data Protection Officer, RPD - responsabile della protezione dei dati)

- Quindi:

l'obbligo scatta indipendentemente dai dati personali oggetto di trattamento, in capo a chi effettua un monitoraggio regolare e su larga scala delle persone fisiche o tratta su larga scala categorie particolari di dati personali (art. 37, par.1).

Nomina DPO

- La designazione del DPO è particolarmente raccomandata per tutti i casi in cui ***le attività di trattamento costituiscano probabili fonti di rischio per i diritti e le libertà delle persone fisiche***, in base a **valutazioni** affidate, nei singoli casi, ai ***Titolari e ai Responsabili***, in attuazione del fondamentale principio *dell'accountability*.

Al Data Protection Officer – DPO - non può e non deve spettare una funzione di tutela degli interessi del Titolare e del Responsabile, ma un ***ruolo esclusivamente dedicato alla protezione dei dati personali***

DPO non ha vincoli

- Il DPO non è incardinato in vincoli gerarchici,
- ha il dovere di agire in modo indipendente
- l'incarico conferito al DPO esterno non deve assumere la forma di un semplice mandato professionale o di un affidamento di servizi.

TITOLARE DEL TRATTAMENTO, RESPONSABILE DEL TRATTAMENTO, DPO

Webgrafia

- *Regolamento (UE) 2016/679*, https://www.garanteprivacy.it/il-testo-del-regolamento, 1 agosto 2018;
- *Gdpr, ecco le vere funzioni del DPO: "attenti, non è un mestiere,*

https://www.agendadigitale.eu/sicurezza/gdpr-attenti-fare-il-dpo-non-e-un-mestiere-ecco-le-sue-vere-funzioni/
di Franco Pizzetti, Professore ordinario di Diritto Costituzionale presso la Facoltà di Giurisprudenza dell'Università di Torino, 25 maggio 2017

- *Gdpr, chi è responsabile di cosa: chiariamo i dubbi diffusi tra le aziende;*
  https://www.agendadigitale.eu/sicurezza/privacy/gdpr-chi-e-responsabile-di-cosa-chiariamo-i-dubbi-diffusi-tra-le-aziende/

di Franco Pizzetti, Professore ordinario di Diritto Costituzionale presso la Facoltà di Giurisprudenza dell'Università di Torino, 18 Apr 2018

Art. 24 Responsabilità del titolare del trattamento

- Il GDPR ruota intorno al concetto *dell'accountability* ,
- alla **responsabilità del titolare del trattamento**
- **L'art. 24 delinea tale figura:**
- **1.Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche,**
- **il titolare del trattamento mette *in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.* Dette misure sono riesaminate e aggiornate qualora necessario.**

Art. 24 par. 2, 3

- 2.Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono *l'attuazione di politiche adeguate in materia di protezione dei dati* da parte del titolare del trattamento.
- 3.L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Le responsabilità del titolare

- Le responsabilità del titolare vanno dalle attività che questi deve svolgere fin dalla fase della progettazione dei trattamenti,
- quindi attività di *privacy by design*,
- *privacy by default*,
- adozione di misure adeguate ad assicurare la sicurezza dei trattamenti

Considerando 74-79

- il titolare deve decidere

❑le misure tecniche e organizzative da adottare in ragione dei rischi che il trattamento (processo) che vuole porre in essere può far correre ai diritti e alle libertà delle persone fisiche.

- I **Considerando che vanno dal 74 al 79** riguardano i ***rapporti con l'eventuale responsabile*** (processor) al quale il titolare (controller) affida una parte o anche tutto il trattamento, che dovrà essere svolto sulla base delle sue istruzioni, in suo nome e sotto il suo controllo (art.28 GDPR).

Considerando 74

- «È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto.
- In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure.
- Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.»

Considerando 78

- «La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento.
- Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default.»

Considerando 78

- «Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali,
- *pseudonimizzare* i dati personali il più presto possibile,
- offrire *trasparenza* per quanto riguarda le funzioni e il trattamento di dati personali,
- consentire all'interessato di *controllare il trattamento* dei dati e consentire al titolare del trattamento di creare
- e migliorare caratteristiche di *sicurezza*. «

Considerando 78

- «In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati.
- I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici.»

Considerando 79

- Il Considerando 79: rapporti tra titolare e responsabile:
- «La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo,
- esigono una **chiara ripartizione delle responsabilità** ai sensi del presente regolamento,
- compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente **con altri titolari** del trattamento o quando l'operazione di trattamento viene **eseguita per conto del titolare** del trattamento.»

Considerando 79

- **Quindi il considerando 79 chiede che siano sempre chiari i ruoli e le responsabilità dei diversi soggetti che intervengono in un trattamento o in un complesso di trattamenti**

Art. 28

- L’art. 28: i rapporti tra titolare e responsabile dei trattamenti devono essere regolati da “un contratto o altro atto giuridico a norma del diritto dell’Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare” (art. 28 paragrafo 3).

- il contratto (o l’atto giuridico adottato) deve vincolare il titolare al responsabile e deve specificare “la materia disciplinata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento”.

Art. 28

- Nell’art. 28 nelle lettere dalla a) alla h) – 8 - sono
- specificati gli obblighi del responsabile nei confronti del titolare.

❑Essi riguardano tutti i diversi aspetti del rapporto tra il titolare e responsabile,

❑le modalità con le quali il responsabile deve trattare i dati per la parte di trattamento a lui affidata dal titolare.

❑il contenuto del contratto o dell’atto giuridico che lega le due figure

Art. 28 Responsabile del trattamento, par. 4

- Quando un responsabile del trattamento **ricorre a un altro responsabile** del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti,
- mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, **gli stessi obblighi** in materia di protezione dei dati contenuti **nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento** di cui al paragrafo 3,
- prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento.

…Art. 28 Responsabile del trattamento, par. 4

- Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale **conserva nei confronti del titolare del trattamento l'intera responsabilità** dell'adempimento degli obblighi dell'altro responsabile.

Sub-responsabili

- Quindi la nomina di eventuali sub-responsabili necessita dell'autorizzazione scritta del titolare,
- che deve esser rinnovata nel caso che subentrino modifiche nei rapporti tra responsabile e sub-responsabile

Titolare

- ***la responsabilità è sempre e solo esclusivamente del titolare***, **non solo per quanto riguarda la *compliance* al GDPR ma anche ogni altro aspetto dei trattamenti posti in essere.**
- Anche se le responsabilità rispetto ai trattamenti sono ripartite tra diverse strutture interne facenti capo a specifici responsabili direttamente dipendenti dal titolare.
- Il titolare resta uno e uno solo e tutti i trattamenti fanno sempre capo a lui e alla responsabilità che su di lui grava.

GDPR - Obblighi generali – Art. 24

- Responsabilità del **titolare del trattamento**
- 1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento **mette in atto *misure tecniche e organizzative adeguate* per garantire, ed essere in grado di *dimostrare*, che il trattamento è effettuato conformemente al presente regolamento**. Dette misure sono riesaminate e aggiornate qualora necessario.
- 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di ***politiche adeguate in materia di protezione*** *dei dati da parte del titolare del trattamento.*

GDPR - Obblighi generali – Art. 24

- 3. L'adesione ai **codici di condotta** di cui all'articolo 40 o a un meccanismo di **certificazione** di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento

DPO

- DPO (o, in italiano, RDP): il **WP29** nel Parere n. 243 del 13 dicembre 2016/5 aprile 2017, aveva affermato che il DPO è una figura non prevista nella Direttiva 95/46
- Ma in molti Stati membri, spesso col consenso delle Autorità garanti nazionali, si era affermata una figura alla quale veniva assegnato il compito di **vigilare in via generale sui trattamenti posti in essere dal titolare**

Capo IV

- Il Responsabile della protezione dei dati personali (DPO) è disciplinato nel Capo IV, tutto dedicato alle **norme relative ai compiti e alle responsabilità del titolare (e del responsabile) dei trattamenti**.

- - è nella sezione quarta del Capo IV: la normativa sul RDP (DPO)
- Mentre la Sezione 1^ è sugli: obblighi generali
- la 2^: sicurezza dei dati
- la 3^: valutazione di impatto
- la 5^:codici di condotta e certificazioni

Titolare del trattamento

- il “centro” del sistema delineato dal GDPR è rappresentato dal **Titolare del trattamento**,
- 1) egli è responsabile della designazione del RDP, compreso l’accertamento delle sue capacità professionali rispetto alle funzioni da svolgere
- 2) il Responsabile dei dati è un “funzione” non un “mestiere”

Quesito al Garante

- E l'Autorità italiana, pronunciandosi su un quesito che le è stato posto (cfr. newsletter Garante privacy n. 43 del 15 settembre 2017), ha affermato che:
- - il RDP deve avere una specifica competenza "***della normativa e delle prassi in materia di dati personali nonché delle norme e delle procedure amministrative che caratterizzano il settore***"
- - deve avere "***qualità professionali adeguate alla complessità del compito da svolgere***" e per settori delicati come quello della sanità, deve dimostrare di avere competenze specifiche rispetto ai tipi di trattamento posti in essere dal titolare

Art. 37.5 REGOLAMENTO (UE) 2016/679

- Infatti
- Art. 37.5 (che richiama all'art. 39) - compiti del RDP:
- **«5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della**
- **conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i**
- **compiti di cui all'articolo 39. «**

Art. 39 GDPR…

- «**Compiti del responsabile della protezione dei dati**
- 1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:
- a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

Art. 39 GDPR…

- b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

… Art. 39

- d) cooperare con l'autorità di controllo; e
- e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
- 2. Nell'eseguire i propri compiti il responsabile della protezione dei dati **considera debitamente i rischi inerenti al trattamento**, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Casi di designazione obbligatoria

- la designazione del DPO è obbligatoria

❑ secondo l'art. 37:

1. per la Pubblica Amministrazione senza eccezioni;
2. per trattamenti che richiedono il monitoraggio regolare e sistematico di dati su larga scala;
3. per i trattamenti riguardano dati personali sensibili (art. 9)
4. per dati relativi a condanne penali e a reati di cui all'art.10 trattati su larga scala

Art. 37:

- Responsabile della protezione dei dati
- **Designazione del responsabile della protezione dei dati**
- 1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:
- a) il trattamento è effettuato da **un'autorità pubblica o da un organismo pubblico**, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

Art. 37:

- b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in **trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio** regolare e sistematico degli interessati su larga scala; oppure
- c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel **trattamento, su larga scala, di categorie particolari di dati personali** di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Ma il titolare…

- il titolare deve adottare tutte le misure organizzative e tecniche adeguate “a garantire ed essere in grado di dimostrare, che il trattamento è effettuato in conformità al Regolamento” (art. 24. primo paragrafo).
- La **designazione di un DPO**, per il quale viene garantita l’indipendenza e i mezzi organizzativi e strumentali necessari,
- aiuta il titolare del trattamento a **dimostrare la sua *compliance*** con quanto previsto dal GDPR

Se non c’è obbligo

- anche laddove il titolare non ha l’obbligo può ritenere opportuno procedere alla nomina del DPO,
- come **ulteriore misura** idonea a dimostrare la conformità dei trattamenti al regolamento
- in tal caso, però è obbligato a rispettare tutta la normativa relativa a questa figura.
- Quindi **non possono essere nominate figure professionali inadeguate o alle quali non siano garantiti i poteri, la posizione di indipendenza e le risorse necessarie previste dalle norme**

Tra le funzioni…

- il DPO svolge anche:
- **funzione di interfaccia** tra titolare e interessati, e
- tra titolare e Autorità garanti
- per questo deve poter operare in modo autonomo ed indipendente presso il vertice dell'organizzazione titolare dei trattamenti (di norma per le imprese il CEO)

- Anche il parere n. 243 del Gruppo art. 29 al punto 4.2., afferma: "qualora il titolare **non concordi con le indicazioni** fornite dal DPO, è necessario che la documentazione relativa alla DPIA (Valutazione di impatto) riporti **specificamente e per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni**".

art. 39 paragrafo 6

- Infine, il DPO può svolgere anche altre funzioni e compiti diversi da quelli propri del suo ruolo, ma spetta al titolare accertarsi *“che tali compiti e funzioni non diano adito a conflitto di interessi”*.

RAPPORTI TITOLARE E RESPONSABILE TRATTAMENTO DATI

45

DOTT.SSA LUANA FIERRO

Webgrafia

- *Regolamento (UE) 2016/679, https://www.garanteprivacy.it/il-testo-del-regolamento, 1 agosto 2018;*
- *GDPR, come devono cambiare i rapporti contrattuali tra titolare e responsabile trattamento dati*
- **di Franco Pizzetti –**
  (professore ordinario di Diritto Costituzionale - Facoltà di Giurisprudenza Università di Torino)
- https://www.agendadigitale.eu/sicurezza/privacy/gdpr-come-devono-cambiare-i-rapporti-contrattuali-tra-titolare-e-responsabile-trattamento-dati/

Responsabile esterno

- La precedente normativa italiana, quindi il Codice italiano per la protezione dei dati personali prevedeva la **figura del responsabile interno all'organizzazione del titolare**, al quale potevano essere delegate specifiche responsabilità anche con effetto verso l'Autorità di controllo e gli interessati.
- L'attuale normativa non consente più questo, il responsabile ex **art. 28 (Responsabile del trattamento)** non può essere una figura che fa parte dell'organizzazione del titolare ma solo **un soggetto ad essa esterna**
-

Responsabile del trattamento

- **il responsabile, da con confondere col titolare - ex art. 28 del GDPR,** può essere solo una figura esterna, distinta e separata dall'organizzazione del titolare, così come chiarito dal 2010 dal **Working Party29** nella sua Opinion

- L'Opinion del Working Party 1/2010, qualifica i diversi soggetti che, in posizioni diverse uno dall'altro, prendono parte alle attività svolte
- Essa aveva delineato la figura del contitolare (oggi all'art. 26 GDPR) non prevista nella precedente Direttiva

Articolo 28
Responsabile del trattamento

- 1.Qualora un trattamento debba essere effettuato per conto del titolare del trattamento,
- quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto **misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti** del presente regolamento
- e garantisca la tutela dei diritti dell'interessato.

Articolo 28
Responsabile del trattamento

- 2.Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento.
- Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche…

Sicurezza dei dati personali Art. 32 - Sicurezza del trattamento

- 1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il ***titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate*** per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
- a) la ***pseudonimizzazione e la cifratura dei dati personali***; 4.5.2016 IT Gazzetta ufficiale dell'Unione europea L 119/51

Sicurezza dei dati personali Art. 32 - Sicurezza del trattamento

- b) la capacità di ***assicurare su base permanente la riservatezza***, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c) la capacità di ***ripristinare tempestivamente la disponibilità e l'accesso*** dei dati personali in caso di incidente fisico o tecnico;
- d) una ***procedura*** per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Art. 32, paragrafo 2, 3

- 2. Nel valutare l'adeguato livello di sicurezza, **si tiene conto** in special modo **dei rischi presentati dal trattamento** che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
- 3. **L'adesione a un codice di condotta** approvato di cui all'articolo 40 **o a un meccanismo di certificazione** approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

Art. 32, paragrafo 4

- 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e ***abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento***, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Art. 36 Consultazione preventiva

- 1. Il titolare del trattamento, prima di procedere al trattamento, ***consulta l'autorità di controllo*** qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il ***trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.***

Art. 36 par. 2

- 2. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un **termine di otto settimane** dal ricevimento della richiesta di consultazione,
- un **parere scritto** **al titolare del trattamento e, ove applicabile, al responsabile del trattamento** e può avvalersi dei poteri di cui all'articolo 58.
- Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto.

Art. 36 par. 2

- L'autorità di controllo **informa il titolare** del trattamento e, ove applicabile, il **responsabile** del trattamento di tale ***proroga***, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione.
- La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

Art. 36 par.3

- 3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:
- a) ove applicabile, le rispettive **responsabilità del titolare** del trattamento, dei **contitolari** del trattamento e dei **responsabili** del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;
- b) le finalità e i mezzi del trattamento previsto;

Art. 36 par.3

- c) le **misure e le garanzie previste per proteggere** i diritti e le libertà degli interessati a norma del presente regolamento;
- d) ove applicabile, i dati di contatto del titolare della protezione dei dati; e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;
- f) ogni altra informazione richiesta dall'autorità di controllo.

Art. 36 par. 4, 5

- 4.Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento.
- 5.Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento **consultino l'autorità di controllo**, e ne ottengano **l'autorizzazione preliminare**, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un **compito di interesse pubblico**, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

Responsabile e titolare

- È l'obbligo del responsabile **assistere il titolare** del trattamento "nel garantire il rispetto degli obblighi di cui dagli articoli da 32 a 36, quindi per:

- misure di sicurezza;
- *data breaches* e segnalazione a Autorità di controllo e agli interessati;
- valutazione di impatto; consultazione preventiva dell'Autorità di controllo nei casi stabiliti dall'art. 36.

Responsabile e titolare

- Il responsabile del trattamento diventa un ruolo il cui svolgimento concorre in modo determinante a definire le caratteristiche delle modalità di trattamento dei dati, al fine di valutare il rischio che il trattamento comporta e adottare le misure adeguate

Titolare e responsabili

- Quindi il titolare, se intende avvalersi anche di responsabili del trattamento, per ***una adeguata valutazione di rischio***
- **e una soddisfacente valutazione di impatto**,
- ***deve conoscere***
  - ***le istruzioni che intende impartire al responsabile***,
  - le **modalità che in concreto questi adotterà** e
  - le **misure che utilizzerà** per garantire che la parte di trattamento a lui affidata non determini una variazione della valutazione di rischio rispetto a come definita dal titolare

Responsabile e titolare

- - il responsabile è tenuto anche a concorrere col titolare, e ad assisterlo per le **segnalazioni di *data breaches***.
- Quindi il contratto o l'atto giuridico vincolante deve:
- porre obblighi chiari al responsabile su tale punto, almeno per la parte di sua competenza,
- e prevedere un dovere specifico di **segnalazione tempestiva delle perdite o alterazioni di dati** effettuatisi nell'ambito dei trattamenti a lui affidati

Contratti con i responsabili

- Quindi nel rispetto del nuovo GDPR il titolare deve decidere da subito se intende avvalersi di responsabili, prima di dare avvio ai trattamenti,
- E deve stipulare da subito i contratti e gli atti giudici vincolanti necessari

Contratti già vigenti

- E per i trattamenti già in corso è opportuno che il titolare ed il responsabile procedano ad una **rivisitazione dei contratti in essere**
- Potrebbe dover essere opportuno modificarne il contenuto,
- affinché essi **contengano obblighi** adeguati ad assicurare che il titolare **possa tempestivamente segnalare** anche perdite di dati verificatesi presso il responsabile

Modifica o rescissione

- Se non fosse sufficiente una modifica dei rapporti contrattuali potrebbe essere opportuno procedere ad una **rescissione** del contratto
- ed all'individuazione di un nuovo responsabile

rapporto tra titolare e responsabile

- Una delle novità del GDPR in materia di misure da adottare:
- il titolare, nel progettare i trattamenti deve tener conto anche dei **contratti stipulati o in corso di stipulazione con i responsabili.**

- Infatti il contenuto di questi contratti, dovendo specificare anche le modalità e le misure che il responsabile si impegna ad adottare, costituiscono una **componente essenziale della valutazione di rischio** che spetta al titolare fare, anche con l'assistenza del responsabile

Responsabile - titolare

- il titolare

❑deve verificare il contenuto degli impegni contrattuali presenti sugli impegni assunti

❑la concreta attività del responsabile

- **il responsabile deve garantire al titolare di poter corrispondere in modo adeguato ai reclami degli interessati**
- **e di esercitare tempestivamente l'obbligo di segnalazione delle *data breches* all'Autorità di controllo.**

DENUNCIA DATA BREACH

- Ci sono 72 ore di tempo per denunciare un *data breach, le quali vengono* calcolate dal momento in cui il titolare viene a conoscenza della perdita o alterazione dei dati,

- Ed è opportuno che il titolare sia in grado di monitorare costantemente la conservazione dei dati,
- perché deve poter individuare nel tempo più breve possibile un'eventuale perdita o alterazione.
-

… DENUNCIA DATA BREACH

- Il responsabile per la sua parte, è tenuto ad assistere il titolare anche sotto questo aspetto.
- Pertanto, bisogna stare attenti ai contratti che hanno ad oggetto l'affidamento della conservazione dei dati a soggetti terzi,
- Es.: i **contratti *cloud***, se necessario devono essere "rivisitati" per assicurarsi che il responsabile che li usa per conservare i dati, sia tenuto a monitorare costantemente la loro integrità
- e se necessario avvisare tempestivamente il titolare.

Fornitori di servizi

- Bisogna prestare attenzione anche **all'attività di fornitori di servizi di trattamento dati affidati a soggetti terzi, che operano come responsabili.**
- Per il considerando 81: "il **titolare** del trattamento dovrebbe ricorrere unicamente a responsabili che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, **affidabilità** e risorse, per **mettere in atto misure tecniche e organizzative** che soddisfino i requisiti del presente Regolamento".

Ricorso ad organizzazioni esterne

- il titolare può far ricorso,
- per l'esecuzione di una parte o anche di tutto un trattamento,
- a strutture e organizzazioni esterne all'impresa, tramite
  - contatti di servizio
  - o atti vincolanti
- che fanno gravare sul terzo l'obbligo di fornire prestazioni adeguate ai trattamenti posti in essere dal titolare

Responsabilità del titolare

- Quindi ricordiamo che il principio prevede (art. 24) che la responsabilità spetti sempre e solo al titolare
- Per questo bisogna avere chiaro chi opera come titolare, ed è dunque **il soggetto al quale spetta dimostrare in ogni momento la conformità dei trattamenti posti in essere *per sua decisione e sotto il suo controllo*, al GDPR,**
- **e chi invece opera *per incarico di questi*, eseguendone le istruzioni e agendo in suo nome.**

Autonomia del responsabile

- Sempre più spesso ci sono in cui il rapporto tra il **titolare e chi esegue** comunque una parte casi del trattamento può essere di **difficile** definizione,
- In quanto **anche il responsabile**,
- (che comunque opera in quanto tale per conto e in nome del titolare)
- può operare con una sua autonomia
- e, per certe fasi della sua attività, soprattutto con riguardo alla sua organizzazione interna e ai trattamenti connessi, **può** anche **assumere la posizione di titolare**

contitolari

- la valutazione di rischio per assicurare la *compliance* al Regolamento può spettare a un unico titolare o essere condivisa dal titolare con altri che, anch'essi, concorrono a decidere, in tutto o in parte, tali modalità.
- Se il potere decisionale relativo alle modalità di svolgimento di un medesimo trattamento è condiviso tra più soggetti, a ciascuno dei quali spetta, **per la sua parte**,

la valutazione di rischio

e la decisione sulle conseguenti misure da adottare, costoro devono essere qualificati non responsabili ex art. 28 ma ***contitolari*** ex art. 26 del GDPR.

Altri soggetti sotto controllo

- Problemi ci sono quando il titolare e gli eventuali contitolari ritengono che una o più delle attività connesse ai trattamenti,
- totalmente o parzialmente possono essere **svolte da altri soggetti** diversi e distinti, operanti **sotto il loro controllo ma non alle loro dipendenze,**
- si pone il problema di definire il rapporto che sussiste tra chi è titolare e chi responsabile,
- gli obblighi che ciascuno dei due assume rispetto all'altro,
- e le specifiche responsabilità del titolare e degli eventuali contitolari verso gli interessati e le Autorità di controllo

Titolare e responsabile

- Quindi bisogna essere sicuri di chi sia il ***titolare*** dei trattamenti di dati
- e verso le Autorità di controllo bisogna indicare con chiarezza chi svolge il ruolo di titolare,
- e dunque rispondere integralmente dei trattamenti posti in essere
- e chi ***quello di responsabile***, e dunque risponde del suo operato direttamente al titolare e solo indirettamente ed eventualmente, ai fini dell'accertamento dei fatti, anche all'Autorità di controllo.